UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,802	12/12/2003	David M. Chess	YOR920030570US1	3904

7590 08/20/2008

Moser, Patterson & Sheridan
Suite 100
595 Shrewsbury Avenue
Shrewsbury, NJ 07702

EXAMINER	
TURCHEN, JAMES R	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
08/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/734,802	**Applicant(s)** CHESS ET AL.	
	Examiner JAMES TURCHEN	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _29 May 2008_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-17 and 23-30_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-17 and 23-30_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claims 1-17 and 23-30 are pending. Claims 1, 7, 16, 17, 23, 29, and 30 are amended.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/29/2008 has been entered.

Response to Arguments

Applicant's arguments with respect to claims 1-17 and 23-30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-17 and 23-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lachman, III et al. (US 2002/0166063, hereafter Lachman) in view of Nakae et al. (US 2004/0172557, hereafter Nakae) and Gong.

Regarding claims 1, 23, and 30:

Lachman discloses a method for automated adaptive reprovisioning of servers under security assault, the method comprising:

detecting a security assault or a possible secuiryt assault on a first server [*paragraph 98, packet sniffing module reads each packet collected during a cycle, each packet being a possible security assault*];

incrementing a counter associated with the first server to account for the security assault or possible security assault [*paragraph 102, the network load increments and decrements with the amount of traffic, an increase in packets increments the network load*];

notifying a human operator if a value of said counter exceeds a maximum limit [*paragraph 103, the attack can be indicated on a GUI when the current load exceeds the threshold*].

Lachman discloses performing countermeasures [*figure 9*], but does not disclose reprovisioning by automatically creating a new server instance with a new server configuration to perform at least one of the tasks performed by said first server, if said value of said counter does not exceed the maximum limit, wherein said new server configuration for said new server instance is selected from a table comprising a plurality of new server configurations, said new server configuration being associated in said table with said value of said counter.

Nakae discloses luring a DOS (denial of service) attack into a decoy unit based on a value and a threshold [*paragraph 191*]. When a DOS attack is not being detected, Nakae discloses sending traffic to a normal server [*paragraph 192*]. Based on this, Nakae also inherently discloses a decision table with two conditions based on the value and the threshold. It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method as disclosed by Lachman with the method for new server configurations as disclosed by Nakae in order to improve the response of a detected assault [*Nakae, paragraphs 19 and 20*].

Lachman and Nakae still do not disclose having multiple configurations within the table. Gong discloses many configuration changes that can take place such as changing the level of access control imposed on clients, degrees of redundancy or isolation, increased sensitivity by the intrusion sensor, or altering the tolerance protocol, the acceptance tests, network connections, or other network characteristics [*column 7 lines 30-43*]. It would have been obvious to one of ordinary skill in the art at the time of invention to modify the table of Lachman and Nakae to include more configuration possibilities as disclosed by Gong in order to minimize the impact of intrusive events [*column 2 lines 33-35*].

Regarding claims 2 and 24:

Lachman, Nakae, and Gong disclose the method of claims 1 and 23, wherein said detecting comprises determining if said first server is a candidate for reprovisioning, because of properties or behavior that suggest its security has been compromised or is likely to be compromised, or its functioning otherwise unacceptably impaired, by a security assault [*Lachman, paragraph 102*].

Regarding claims 3 and 25:

Lachman, Nakae, and Gong disclose the method of claims 1 and 23, wherein said reprovisioning comprises automatically bringing up said new server instance, or otherwise making available said new server instance to customers or other users of said first server [*Nakae, paragraphs 192 and 193*].

Regarding claims 4 and 26:

Lachman, Nakae, and Gong disclose the method of claims 1 and 23, further comprising bringing down said first server prior to said reprovisioning [*Nakae, figure 1 and paragraphs 192 and 193, when the reprovisioning takes place, the first server is brought down (server 401) and traffic is moved to the second server (decoy 2)*].

Regarding claims 5 and 27:

Lachman, Nakae, and Gong disclose the method of claims 1 and 23, wherein said new server instance brought up in said reprovisioning differs from said first server in at least one parameter [*Nakae, figure 1, the decoy unit 2 is in a different location than server 401 as well as having a different internal IP address*].

Regarding claims 6 and 28:

Lachman, Nakae, and Gong disclose the method of claims 1 and 23, wherein a difference between said new server instance and said first server is responsive to whether or not other security incidents have been detected in a network to which said servers are coupled [*Gong, column 6 line 63-column 3, the intrusion sensors detect security incidents within the network, column 7 lines 30-43, a new configuration is used*].

Regarding claims 7 and 29:

Lachman, Nakae, and Gong disclose the method of claims 1 and 23, wherein a difference between said new server instance and said first server is responsive to a nature of any other security incidents that have been detected in a network to which said servers are coupled [*Gong, column 7 lines 30-43, the configurer receives information from intrusion sensors, acceptance monitors, ballot monitors, and proxy servers and generates new configurations as necessary*].

Regarding claim 8:

Lachman, Nakae, and Gong disclose the method of claim 1, wherein a difference between said new server instance and said first server is responsive to a probable compromise or a functional impairment observed in said detection [*paragraph 98, packet sniffing module reads each packet collected during a cycle, each packet being a probable compromise*].

Regarding claim 9:

Lachman, Nakae, and Gong disclose the method of claim 1, wherein a difference between said new server instance and said first server includes a version of server software used by said servers [*Nakae, paragraph 195, the decoy unit may be completely set as a mirror server of the server or may be set such that it provides only general services (thus it is a different version than the original server)*].

Regarding claim 10:

Lachman, Nakae, and Gong disclose the method of claim 1, wherein a difference between said new server instance and said first server includes a version of operating system software used by said servers. Examiner takes official notice that patching is well known in the art to overcome known vulnerabilities. The claim would have been obvious because “a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense.”

Regarding claim 11:

Lachman, Nakae, and Gong disclose the method of claim 1, wherein a difference between said new server and said first serer includes a version of network connectivity software used by said servers [*Gong, column 7 lines 30-43, altering network connections or network characteristics*].

Regarding claim 12:

Lachman, Nakae, and Gong disclose the method of claim 1, but they do not disclose wherein a difference between said new server instance and said first server instance includes a strength of encryption used by said servers. Examiner takes official notice that increasing the strength of encryption would result in a more secure communication. The claim would have been obvious because “a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense.”

Regarding claim 13:

Lachman, Nakae, and Gong disclose the method of claim 1, wherein a difference between said new server instance and said first server includes a degree of function offered to users by said servers [*Gong, column 7 lines 30-43, configurer changes the level of access control imposed on clients*].

Regarding claim 14:

Lachman, Nakae, and Gong disclose the method of claim 1, wherein said new server instance brought up in said reprovisioning differs from said first server only if more than a fixed number of instances of probable server compromise have been observed [*Gong, column 7 lines 30-37, based on the information received the reconfigurer generates new configurations for the system; column 6 lines 63-column 7 line 28, a probable server compromise has been detected*].

Regarding claim 15:

Lachman, Nakae, and Gong disclose the method of claim 1, wherein a difference between said new server instance and said first server is responsive to a number of probable server compromises that have been observed [*Gong, column 7 lines 30-37, based on the information received the reconfigurer generates new configurations for the system; column 6 lines 63-column 7 line 28, a probable server compromise has been detected*].

Regarding claim 16:

Lachman, Nakae, and Gong disclose the method of claim 1, wherein said server comprises a computer providing services through a network [*it is inherent that a server provides services through a network*].

Regarding claim 17:

Lachman, Nakae, and Gong disclose the method of claim 1, wherein said server comprises a program running on a network-coupled computer, providing services through a network [*it is inherent in servers that a computer program is running on a computer and providing services through a network*].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES TURCHEN whose telephone number is (571)270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571)272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139